Remarks

Claims 1-26 are pending and at issue. Of the claims at issue, claims 1, 10, 18, and 25 are independent.

The applicants have carefully considered the Office action mailed on January 31, 2007. In the Office action, claims 1, 5-10, 14-18, and 22-26 were rejected as anticipated by Griffin et al (US 7,076,655) and claims 2-4, 11-13, and 19-21 were rejected as unpatentable over Griffin in view of Fish et al. (US 2003/0110370). In view of the following remarks, reconsideration of the application and allowance thereof are respectfully requested.

Claim 1 recites, *inter alia*, a method of booting a processor system, the method comprising accepting a selection of a desired operating system to be booted, accepting a user credential associated with a user who has selected the desired operating system to be booted, determining if the user credential corresponds to the desired operating system to be booted, and enabling booting of the desired operating system if the user credential corresponds to the desired operating system.

Griffin is directed to a method for verifying the integrity of a computing environment. According to Griffin, a compartment within a host operating system runs a virtual machine application. The virtual machine application, in turn, runs a guest operating system. The guest operating system (also referred to as a computing environment) runs at least one process to obtain integrity metrics for making a determination as to whether an environment (i.e., an operating system) is a trusted environment. At any point thereafter, a user requests demonstration of the integrity of the computing environment through a trusted device. The trusted device supplies integrity metrics associated with the computing environment (i.e., an operating system) and the metrics are compared against expected values. If the comparison is successful, the computing environment is considered a trusted environment.

The Office action asserts that Griffin, col. 12, lines 45-54, describes enabling booting of a desired operating system if the user credential corresponds to the desired operating system. However, reliance on this portion of Griffin for such teaching is misplaced. Contrary to the contentions in the Office action, Griffin states:

> A user is provided an external label for a computing environment. The computing environment passing the indirect integrity challenge provides internal identity, and compartment identification is completed with the external label corresponding with the computing environment. The user then confirms the external label provided in the compartment identification matches the expected computing environment.

(Griffin, col. 12, lines 45-54). In other words, Griffin describes a user evaluating a computing environment (i.e., an operating system) running in a compartment of a host operating system. The user receives the integrity challenge results and determines if the computing environment matches the desired computing environment. Thus, Griffin teaches evaluating a previously-booted operating system. Griffin does not, however, describe the evaluation of the user credentials or the booting of the desired operating system upon verification of the user credentials; instead, Griffin describes the operating system evaluation, not user evaluation.

Furthermore, Griffin does not describe the booting of a selected or desired operating system. To the contrary, in Griffin, the computing environment selected by the user is a process already running in a compartment of a host operating system and would not need to be booted when the user selects the computing environment.

The Office action further asserts that Griffin, col. 14, lines 39-67, describes enabling booting of the desired operating system if the user credential corresponds to the desired

operating system. However, reliance on this portion of Griffin for such teaching is misplaced. Contrary to the contentions in the Office action, Griffin states:

> A trusted computing environment is provided by using a trusted device to verify that a guest operating system has booted in a trusted manner. By repeating this process and running multiple guest operating systems, multiple trusted computing environments can be provided. A first application can run in a first of the computing environments, whilst a second application can run in a second of the computing environments, where the first and second applications are mutually incompatible or one does not trust the other. A user can verify the integrity of one computing environment without reference to the integrity of any other computing environment. Each computing environment has an associated set of one or more integrity metrics which do not include or depend on information about any other computing environment. A method is provided allowing the user (challenger) to confirm that the integrity information corresponds to the expected computing environment.

(Griffin, col. 14, lines 39-67). In other words, this portion of Griffin describes a method to verify that an operating system has booted in a trusted environment. Griffin then describes that a user may verify the integrity of a computing environment without disturbing other computing environments and allowing the user to confirm the computing environment is the desired computing environment. Griffin does not, however, describe the evaluation of the user credentials or the booting of the desired operating system upon verification of the user credentials; instead, Griffin describes the verification of the computing environment after booting to provide a multiple trusted computing environments simultaneously. The user selects a computing environment and may issue an integrity challenge to verify the computing environment is the desired computing environment. Furthermore, Griffin does not describe the booting of a selected operating system in response to the user credentials

being evaluated; instead, the user of Griffin selects the computing environment after the computing environment had been previously booted.

Therefore, Griffin does not describe or suggest enabling booting of the desired operating system if the user credential corresponds to the desired operating system. Accordingly, for at least the forgoing reasons, claim 1 and all claims depending therefrom are in condition for allowance.

Independent claims 10 and 18 include recitations directed to enable booting of the desired operating system if the user credential corresponds to the desired operating system. Therefore, for at least the forgoing reasons related to claim 1, claims 10 and 18 and all claims depending therefrom are in condition for allowance.

Claim 25 recites, *inter alia*, an apparatus to control selection of operating system booting, the apparatus comprising a permissions table storing user credentials and boot objects corresponding to the user credentials, and a user verification segment coupled to the permissions table and accepting a selection of a desired operating system to be booted and further accepting a submitted user credential associated with a user who has selected the desired operating system to be booted, the user verification segment determining if the submitted user credential is authorized to boot the desired operating system.

The Office action asserts that Griffin, col. 5, lines 42-50, describes a user verification segment coupled to the permissions table and accepting a selection of a desired operating system to be booted and further accepting a submitted user credential associated with a user who has selected the desired operating system to be booted, the user verification segment determining the submitted user credential is authorized to boot the desired operating system. Griffin does not describe or suggest a user verification segment determining the submitted user credential is authorized to boot the desired operating system. However, reliance on this

portion of Griffin for such a teaching is misplaced. Contrary to the contentions in the Office action, Griffin states:

> The hardware may also comprise a trusted user interface for performing communication with a user device such as a smart card held by the user. The trusted user interface allows the user to perform trusted communications with the trusted device in order to verify the integrity of the computing platform.

(Griffin, col. 5, lines 42-50). In other words, this portion of Griffin describes a hardware device that communicates to a user device, thus allowing the user device to verify the integrity of the computing platform (i.e., operating system). Griffin does not describe a permissions table nor does Griffin describe a user verification segment that determines if the user credentials are authorized to boot the desired operating system. Thus Griffin teaches a hardware device capable of communicating with a user device and providing a communication path for the user to verify the integrity of the computing platform. Griffin does not, however, describe a permissions table or verifying that the user credentials have been evaluated prior to booting of the selected operating system.

Furthermore, the Office action asserts that Griffin, col. 10, lines 1-10, describes a user verification segment coupled to the permissions table and accepting a selection of a desired operating system to be booted and further accepting a submitted user credential associated with a user who has selected the desired operating system to be booted, the user verification segment determining the submitted user credential is authorized to boot the desired operating system. However, reliance on this portion of Griffin for such teaching is misplaced. Contrary to the contentions in the Office action, Griffin states:

> For a local user, a secure channel is provided such as by using a trustworthy user interface and /or by using a token such as a smart card. A remote user establishes a secure channel such as

> by performing authentication of the computing platform, ideally using a signature from the trusted device. Here again, the user optionally employs trusted hardware, such as the user's own client platform, a PDA, mobile phone or other device, optionally in co-operation with a smart card or other token. Preferably includes establishing the authentication and authorization of the user.

(Griffin, col. 10, lines 1-10). In other words, this portion of Griffin describes the provisioning of a secured channel allowing a user to communicate to perform integrity challenges of the computing platform (i.e., operating system). Griffin does not, however, describe a user verifying the user credentials prior to the booting the selected operating system. Thus, Griffin teaches providing a secure channel for a user to evaluate the integrity of a previously running operating system. The computing device selected is not booted after the user has selected the computing platform, nor is the user credentials evaluated to determine if the user has permissions to boot the desired operating system.

Still further, the Office action asserts that Griffin, col. 10, lines 43-45, describes a user verification segment coupled to the permissions table and accepting a selection of a desired operating system to be booted and further accepting a submitted user credential associated with a user who has selected the desired operating system to be booted, the user verification segment determining the submitted user credential is authorized to boot the desired operating system. However, reliance on this portion of Griffin for such teaching is misplaced. Contrary to the contentions in the Office action, Griffin states that an apparatus and methods described above provide integrity information concerning a selected one of the multiple computing environments. (Griffin, col. 10, lines 43-45). In other words, Griffin teaches the ability of a user to perform integrity challenges of a selected operating system. Thus, Griffin teaches evaluating a previously-booted operating system. Griffin does not, however, describe

the evaluation of user credentials or the booting of the selected operating system based on an evaluation of user credentials.

Next, the Office action asserts that Griffin, col. 10, lines 53-58 describes a user verification segment coupled to the permissions table and accepting a selection of a desired operating system to be booted and further accepting a submitted user credential associated with a user who has selected the desired operating system to be booted, the user verification segment determining the submitted user credential is authorized to boot the desired operating system. However, reliance on this portion of Griffin for such teaching is misplaced. Contrary to the contentions in the Office action, Griffin states that the user issues a request for verification of the integrity of a computing environment, suitably in the form of an integrity challenge. (Griffin, col. 10, lines 55-58). In other words, this portion of Griffin describes the user performing an integrity challenge of a previously booted operating system. Griffin does not, however, describe or suggest a user verification segment determining the submitted user credential is authorized to boot the desired operating system; instead, Griffin describes operating system evaluation, not user credential evaluation.

Finally, the Office action asserts that Griffin, col. 12, lines 12-22, describes a user verification segment coupled to the permissions table and accepting a selection of a desired operating system to be booted and further accepting a submitted user credential associated with a user who has selected the desired operating system to be booted, the user verification segment determining the submitted user credential is authorized to boot the desired operating system. However, reliance on this portion of Griffin for such teaching is misplaced. Contrary to the contentions in the Office action, Griffin states:

> The supplied_externaldata field can be used as in the established system as a defen[s]e against a replay attack, and the compartment_ID field is used to identify the received

> integrity information as being specific to a particular computing environment. The compartment_ID field is compared against an expected value, to confirm that the received integrity information corresponds to the expected computing environment. That is, the integrity information provided to the user is identified as being specific to the computing environment of interest to the user.

(Griffin, col. 12, lines 12-22). In other words, Griffin describes a system to provide an external label attached to a compartment identifier, thereby allowing the user to identify the computing environment as being the expected computing environment. Griffin does not, however, describe the user credentials being evaluated prior to the booting of the selected operating system; instead, Griffin describes operating system evaluation, not user credential evaluation. Accordingly, for at least the forgoing reasons, claim 25 and all claims depending therefrom are in condition for allowance.

Conclusion

The applicants respectfully submit that all claims are in condition for allowance. Reconsideration of the application and allowance thereof are respectfully requested. If there is any matter that the examiner would like to discuss, the examiner is invited to contact the undersigned representative at the telephone number set forth below.

Respectfully submitted,

HANLEY, FLIGHT & ZIMMERMAN, LLC
150 South Wacker Drive
Suite 2100
Chicago, Illinois 60606

Dated: **April 30, 2007**

Mark C. Zimmerman
Reg. No. 44,006
Agent for Applicants
312.580.1020